

# IR Key Programmer



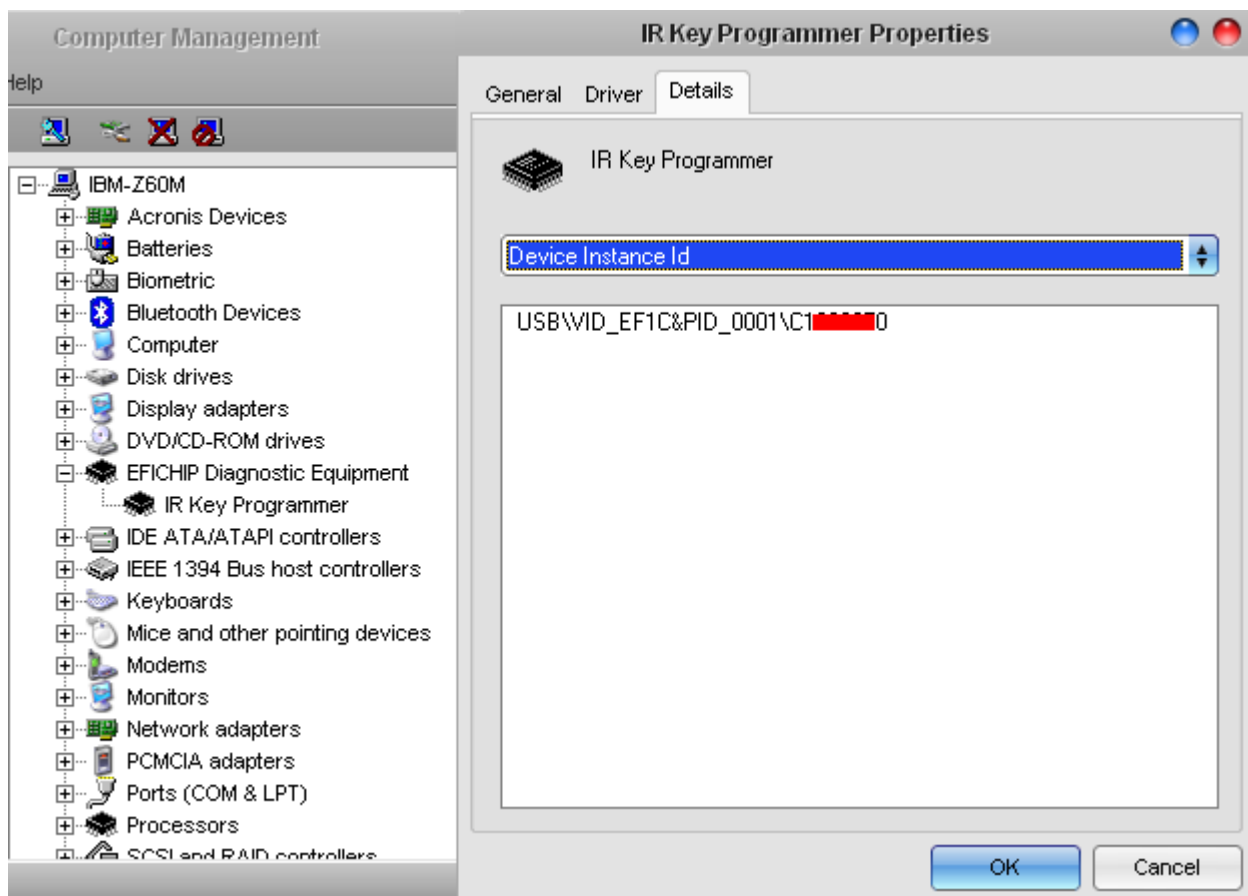
## User Manual

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications.

# Installation

All required software and drivers should be provided by our representatives. If not so, please, request them by Your device serial number. It is visible even with no drivers installed, using built-in Windows applications.

Open Device Manager by right-clicking “My Computer” and after that click “Properties” - “Hardware” - “Device Manager”. Select “IR Key Programmer-Properties”. Select “Details” tab, “Device Instance id”.

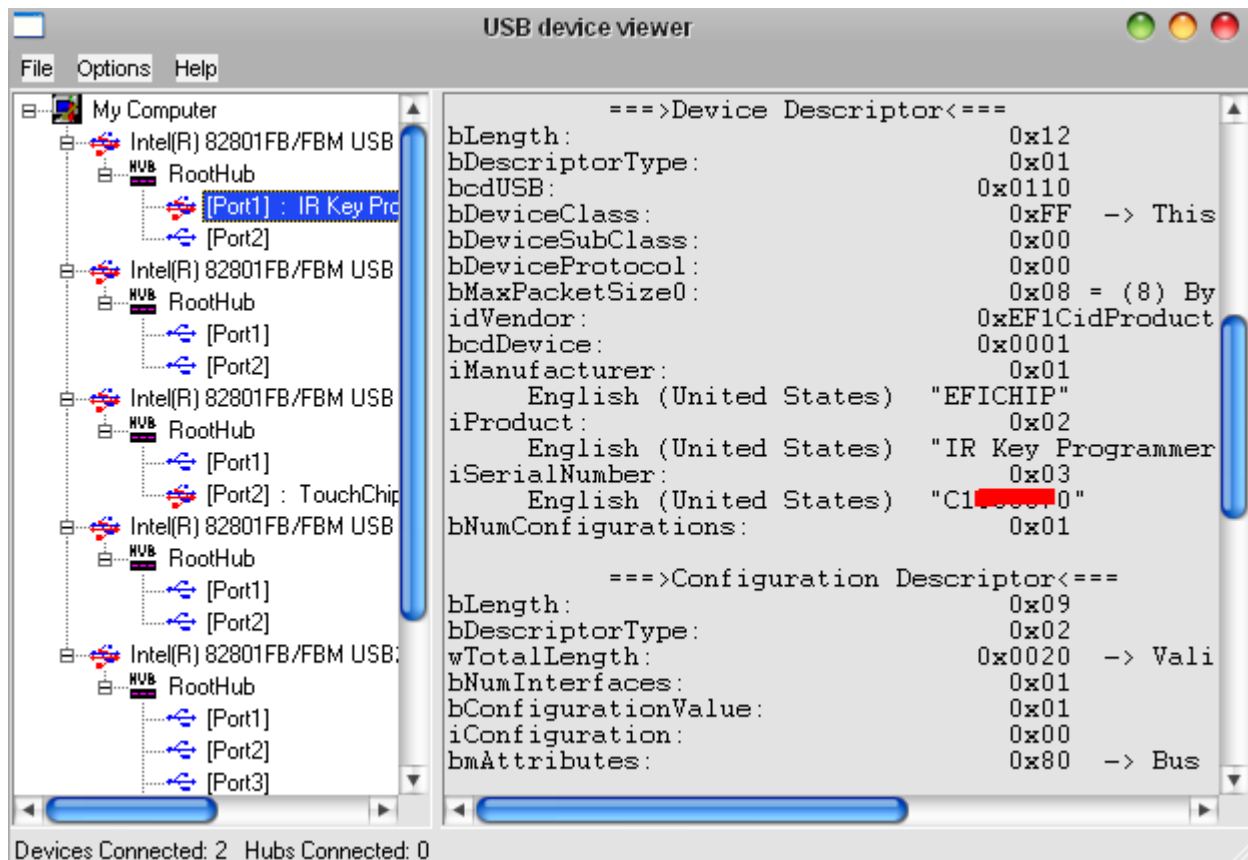


Value, marked with red color on above screenshot is Serial Number of Your device.

Example here is for Windows XP, but for Windows Vista or Windows 7 it is similar.

Choice of operating system is up to You, but Windows XP is always recommended for it's native compatibility with most of USB devices, used for hardware and engineering tasks. Anyway, stable version of USB libraries are provided by Microsoft for Windows Vista and Windows 7.

There are many applications, which are able to show information for USB devices. Official software for such tasks provided by Microsoft Corporation is UVCView.x86.exe. Running it with “Show Config Descriptors” option enabled gives required information. Older USBView.exe configured in same way, gives same result.



Value, marked with red color on above screenshot is Serial Number of Your device.

Provide that Serial Number to our representative and You will receive compatible software. Have in mind, that software is compiled for Your device, hence using incompatible, patched, modified or third-party software may lead to undesirable consequences. Always use trusted providers only!

After installing drivers, software is ready to use. If it doesn't start, probably You do not have device plugged into USB port or driver's installation failed. Application starts only if compatible hardware is connected. IR Key Programmer is powered by USB, so no external power supply is required.

## Instructions

Click “Read” with inserted MB Key into IR Key Programmer or with NEC/Motorola MCU soldered to small adapter board connected aside. Adapter will be automatically recognized and will prevail over IR mode. Always note, that MCU adapter board, connected to IR Key Programmer disables it's IR slot, and even if MB Key is placed there, it will not be recognized, neither will obstruct MCU adapter operation.

Do not remove MB Key from IR Key Programmer when task is completed – keeping it there for long time doesn't causes overheating of inductors, which powers the key. Of course if You are done with Your job, MB Key could be removed at any moment, but if You intend to perform more tasks on it, IR Key Programmer is safe and convenient place for it, since MB Key is powered only when operated.

On completion of task screen will look like:

The screenshot shows the 'IR Key Programmer' software window. It contains several sections for configuring and programming a key:

- Top Section:** Fields for 'Key' (1), 'Status' (14EC), 'SSID' (28118795), 'Ver' (57), and 'Life' (196596). A 'Decrement' button is next to 'Ver', and a 'Read' button is next to 'Life'.
- Frequency and User Info:** 'Frequency' is set to 512 MHz. 'User Info' is 0123456789AB, with a 'Write' button. 'Extra Info' is BA9876543210. 'Battery %' is 0.
- NEC Section:** Includes 'Erase', 'Load', 'Write', and 'Activate' buttons. A 'Power' section has 'ON' and 'OFF' buttons.
- Motorola Section:** Includes a dropdown for '051', 'Load', 'Write', and 'Activate' buttons.
- Fixed Password and Initial Hash:** Fields for 'Fixed Password' and 'Initial Hash' with a 'Random' button and a 'Read' button.
- Bottom Section:** Fields for 'Key' (1), 'Status' (04FC), 'SSID', 'Ver' (NEC), and 'Life' (196607). A 'Do it!' button is at the bottom right.

Starting from left top, You could find following data:

“Key” - Key number. Car has total eight keys and this information helps differentiate current one from the others in the set. Also personalized settings of seats, mirrors, steering wheel, etc... are linked to this number.



“Status” - hexadecimal representation of MB Key internal state of operation. Two bytes completes to number of 0x100 (0x14 + 0xEC=0x100). It is form of data protection, and if check-sum fails, MB Key becomes inoperative. Short description of most common Status digits are given below:

- 0000 - MB Key is blank (erased state of Key with Motorola processor).
- 21DF - MB Key is prepared (Key accepts only encrypted data).
- 04FC - MB Key is programmed, but not activated.
- 05FB - MB Key is programmed, but not activated.
- 14EC - MB Key is activated and fully functional.
- 15EB - MB Key is activated and fully functional.
- 0CF4 - MB Key for service purposes (so called “Green Key”).

“SSID” - hexadecimal representation of MB **S**ystem **S**erial **I**dentification. Matches key to **E**lectronic **I**gnition **S**witch, **I**nstrument **C**luster **M**odule, **C**entral **G**ate**W**ay, etc...

“Ver” - version of software, contained in MB Key's MCU.

“Life” - remaining starts counter – it is same as “Life” counter of EIS hashes, and both decrement simultaneously when MB key is inserted in EIS. Starting value is 196607 when MB key is new and decrements when MB key is used. Differences in “Life” counters of EIS and MB key are rare, but happens and this may lead to car unable to start if key counter is bigger than EIS hash counter.

**Solution is to make key counter same or little lesser then EIS counter!!!**

For this purpose You should click button “Decrement” as many times as You need. This process is automated with Extended functionality of software – read further for additional instructions. This function emulates inserting key to EIS with all data being exchanged as car does. Do not “play” with this button – if key counter becomes too lesser than EIS hash counter key will become nonoperational, which may lead to expensive consequences, depending on car model.

“Frequency” - this helps identify frequency range of key and hence it's market – 315Mhz is USA standard, 433 MHz is EU standard and custom 512 MHz.

“User Info” - not available on all key's software versions – gives service information. You could change data using “Write” button right next to the field.

“Extra Info” - not available on all key's software versions – gives service information. You could change data using “Write” button left prior to the field.

For above “Info” fields You could edit data in fields to whatever suits Your needs, but note that data might means something to MB dealer / workshop.

“Battery” - percentage of remaining capacity of MB key internal battery.

Except reading capabilities, as name of the product implies, You could also program keys. Motorola 68HC05E6 MCUs You are able to read / write / erase with additionally available adapter boards. Both 2 MHz and 4 MHz version are supported and they could be read / written / erased also on-board without desoldering. See Appendix B at the end of this document for further instructions how to connect Motorola to IR Key Programmer.

Same applies to NEC MCUs – You could read / write / erase with additionally available adapter boards for both 2 MHz and 4 MHz versions if processor is desoldered from key's PCB. Available on-board operation without desoldering MCU is only erasing. Different erasing algorithm is implemented, which allows to use fewer wires than competitive products, easing whole process and minimizing risk of MCU's pins damage. See Appendix A at the end of this document for further instructions how to connect NEC to IR Key Programmer.

When key is ready for erasure, just click button “Erase” and appropriate message will appear, indicating operation in progress.

Erasure sequence will be performed and result will be indicated. If You solder wires to NEC MCU while it stays soldered on Key PCB or simple erasure sequence gives no result, then repeated (dummy 😊) erasure sequence could be performed, by writing „Endless!“ in the text field and then clicking button „Erase“:



Endless erase sequence will be started, which guarantees at some point, that You will have fully erased MCU. Current progress is indicated in text field. At any moment erasing procedure could be terminated by clicking „Stop“ button:



If processor is soldered on adapter board, software checks success of erasure (except in „Endless!“ dummy mode 😊) and upon completion of it, You will be able to read processor for confirmation. It is always advisable to solder NEC on adapter for guaranteed results. Not only because of golden plated adapter PCB, which guarantees proper contact and long life of board, but also following processes of programming, activating, Life decreasing operations are faster with adapter. Also if You program wrong file into key it is very easy to erase it and reprogram with correct dump.

If You need to repair Key with corrupted radio trimming bytes, then solder NEC processor on appropriate adapter board, write „Radio!“ in the text field and then click button „Erase“. Wait patiently 😊

Just after all tasks are finished and MCU is prepared for use in car, You could solder it back to key's PCB and make a final reading via IR before using with car.  
**For both Motorola and NEC “Read” / “Write” are available via IR also !!!**

**Always connect and disconnect adapter boards to programmer when USB cable is not plugged in !!!  
Serious damages could occur if IR Key Programmer is powered on while adapter board is being attached or removed !!! Do not avoid this warning !!!**

When processor is erased and You click “Read” screen looks like:

The screenshot shows the 'IR Key Programmer' window. At the top, there's a header bar with the title and standard window controls. Below it, the interface is divided into several sections. The top section has fields for 'Key' (dash), 'Status' (8080), 'SSID' (dashes), 'Ver' (57), and 'Life' (dashes), with a 'Read' button. The middle section has 'Frequency' (512 MHz), 'User Info' (0100456789AB), 'Extra Info' (BA9876543210), and 'Battery %' (0), with a 'Write' button. Below this, there are sections for 'NEC' and 'Motorola' protocols, each with 'Erase', 'Load', 'Done.', 'Write', and 'Activate' buttons. To the right of these is a 'Power' section with 'ON' and 'OFF' buttons. At the bottom, there's a 'Fixed Password' field with a 'Random' button and an 'Initial Hash' field with a 'Read' button. The very bottom section has fields for 'Key' (1), 'Status' (04FC), 'SSID' (blank), 'Ver' (NEC), and 'Life' (196607), with a 'Do it!' button.

Note that fields “Key”, “SSID” and “Life” should be blank (showing dashes) and “Status” field should show inoperative state of key.

For key's dump calculating, You could use bottom section of software or continue with solution currently in use by You.

Dump generating for MB IR Key requires several important fields to be filled with desired data - they will be explained in details below:

“Key” - read explanations on page 4. You should select the key line, You want to generate.

“Status” - read explanations on page 5. In general, if You will generate dump for NEC key, status should be 04FC. But if You are programming Motorola key on adapter board, You could generate 14EC key for direct programming to EPROM of processor. Your experience should lead You for choosing best way of programming Motorola keys – either via IR or via PCB.

“SSID” - read explanations on page 5.

“Ver” - read explanations on page 5.

“Life” - read explanations on page 5.

“Fixed password” - this is so called “EIS password” - 8 unique bytes.

For Motorola-based EIS units it depends on the software, You are using to read EIS dump, to find exact place of those 8 bytes in EIS dump. For different EIS models also exact location is different. You have two options when generating key – read the EIS and take password bytes from the dump, or generate Your own sequence of 8 bytes for key and put these bytes into EIS dump. You could change data using “Random” button right next to the field or enter Your own choice. After that, these bytes You should program to EIS, using corresponding equipment.

For NEC-based EIS units, You could obtain “Fixed password” by reading it from key if it has ROM version 57. Please, read further for instructions.

“Initial hash” - 8 bytes unique to each EIS key line. If You read EIS dump, You will not find those 8 bytes. If You choose to generate key for existing EIS, without modifying it's EPROM, then these 8 bytes could be obtained by available servers or standalone software.

But if You choose to generate Your own sequence of 8 bytes for key and put these bytes into EIS dump, You could change data using “Random” button left next to the field or enter Your own choice. After that 8 bytes, from location 0x73 in generated dump, You should program to EIS, using corresponding equipment. For different EIS models also exact location is different. Also for different models MB, implementing FBS3 security feature, it might be necessary to program not only EIS, but also rest of the FBS3 components present in the car – EVL, ECU, ESL, ISM, etc...

Next step is writing new data. Appropriate button will be activated after loading key dump. If You are working with Motorola MCU, please, select type of key dump – drop-down menu is available corresponding to last three digits of MCU marking. In example if marking is “MA 567 880 011” select 011 before loading. Software recognizes most of key dumps formats. If You experience troubles loading data, please, contact us for upgrade. If data is loaded correctly corresponding fields will show values from dump and “Write” button will be activated.

Clicking it will produce screen like this:

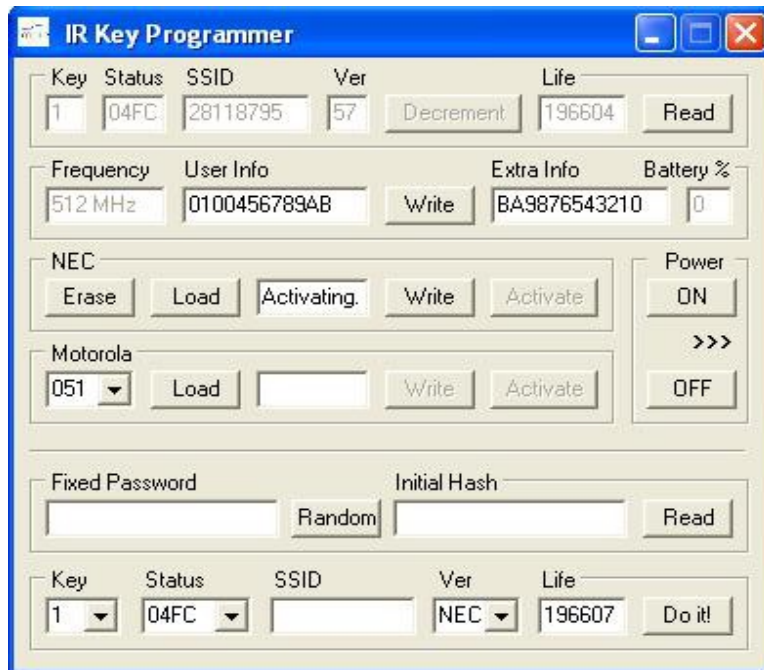
Upon completion You could activate that key if it will be used as replacement of existing / lost key. If You are programming new key for that EIS, then skip this step. Key will be activated automatically when first inserted into EIS.

---

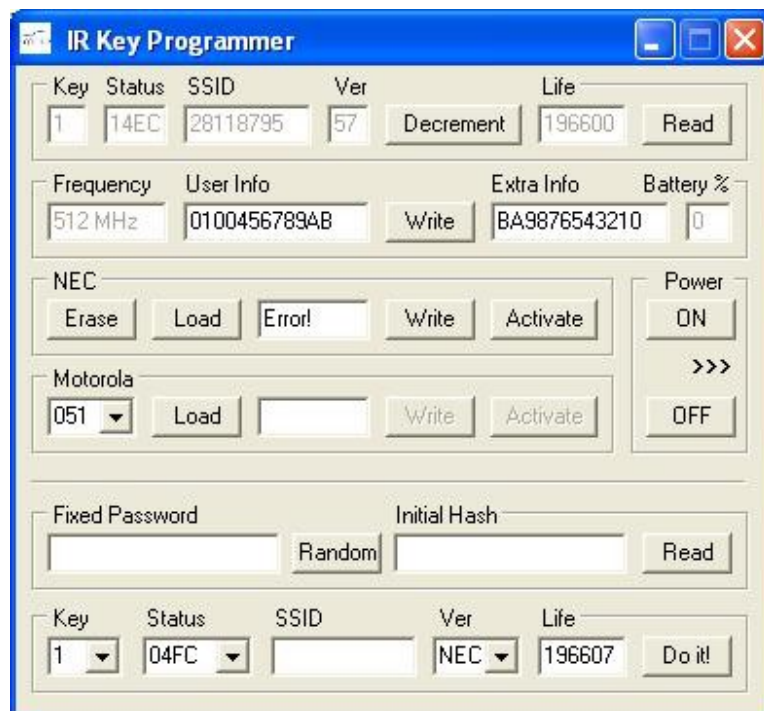
**Remark:** Two buttons in section “Power” are turning On and Off inductor of IR Key Programmer. With their help You could check if inductive coil inside MB key has malfunctioned or is operative. Just click “ON” button and measure voltage across inductor. Or if key is not disassembled, press LOCK / UNLOCK button – if key LED blinks this means coil has failed. Click “OFF” when completed.

**Do not hold “ON” function for long time - overheating could appear !!!**

If You choose to activate the Key, instead of car (do it only if You are familiar with MB key preparation process and how car accepts the Key) press “Activate”:



Despite the message, that software produces after completing (wait patiently until button changes from shaded to normal state) check the result by clicking “Read” button at upper right corner:



If the key You just programmed has ROM version 57, You could check the writing results by reading “Fixed Password” and “Initial Hash” You just wrote to it.

Click “Read” button, right next to “Initial Hash” field – that operation is not necessary to perform if writing process was terminated with message “Done.” - it is for Your fun only.

But “Read” button helps You to read “Fixed Password” and “Initial Hash” of Key, not only You programmed, but also Key, which is original from car. That is the way to obtain this such important “EIS Password” commented above, which will help You to prepare new Keys for that car or adapt Electronic Steering Lock for W204/W207 series. For further processing of EIS password and using it for ESL-adaptation, please, contact our sales representatives for corresponding ESL programming hardware and software.

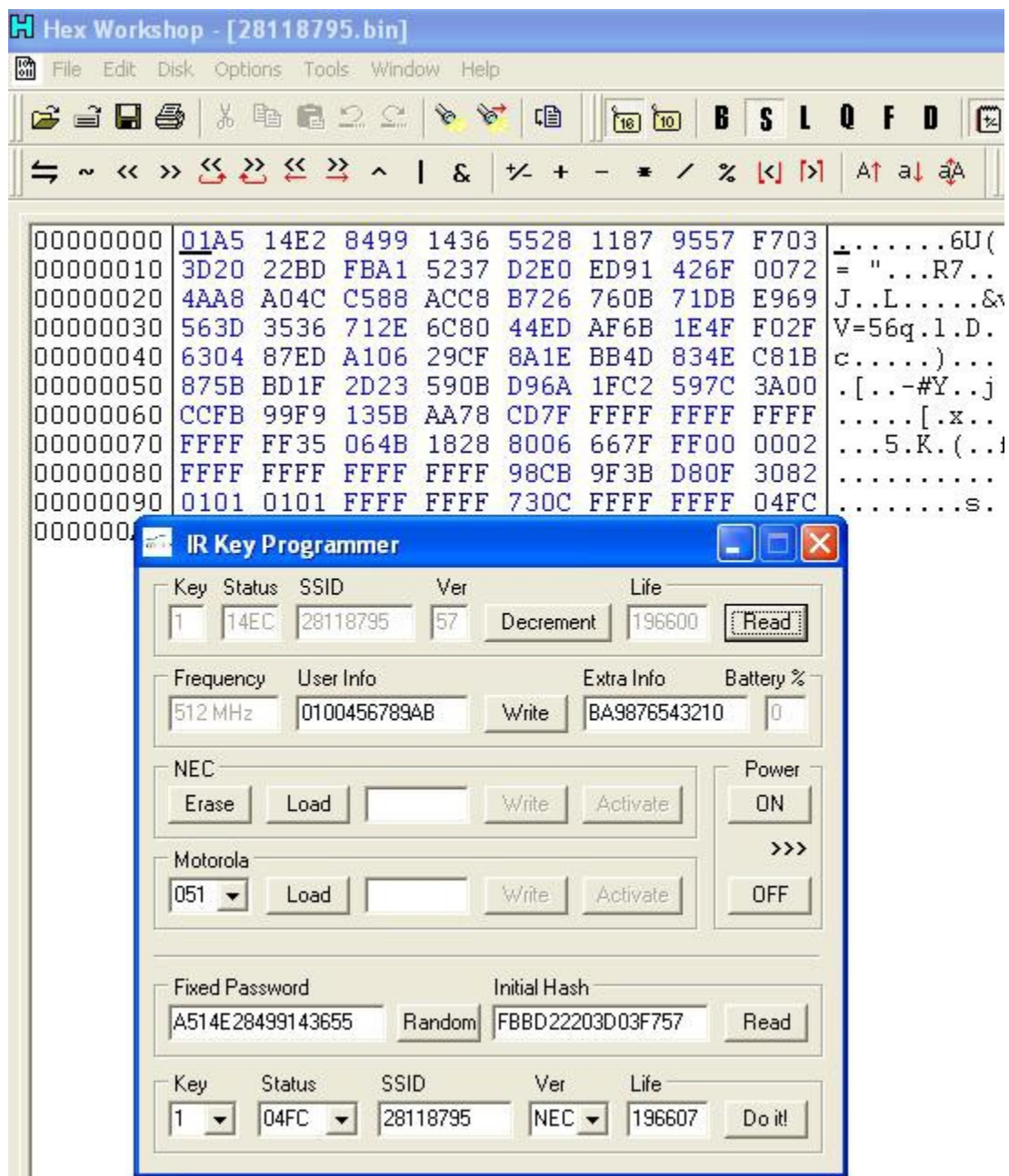
The reading process is fully automated and safe. It doesn't change the Key content, so you do not need to perform any additional tasks after reading. When it completes (in several seconds – it's not an instant reading) You could remove original Key NEC MCU from adapter board (pay attention to the fact, that for v.57 You has special adapter board in the set, which is different that the others provide for 2 MHz and 4 MHz NEC MCUs) and proceed further with erasing/writing another one as already described above.

Click “Read” and You get:

The screenshot shows the 'IR Key Programmer' application window. It features several sections for key programming and reading. At the top, there's a table with columns: Key (1), Status (14EC), SSID (28118795), Ver (57), Life (196600), and a 'Read' button. Below this is a section for 'Frequency' (512 MHz), 'User Info' (0100456789AB), 'Extra Info' (BA9876543210), and 'Battery %' (0), with a 'Write' button. The next section has two rows: 'NEC' with buttons 'Erase', 'Load', 'Error!', 'Write', and 'Activate'; and 'Motorola' with a dropdown (051), 'Load', 'Write', and 'Activate' buttons. To the right of these is a 'Power' section with 'ON' and 'OFF' buttons. The bottom section is for reading, with fields for 'Fixed Password' (with a 'Random' button) and 'Initial Hash' (with a 'Reading...' button and a 'Read' button). At the very bottom, there's another table with columns: Key (1), Status (04FC), SSID (empty), Ver (NEC), Life (196607), and a 'Do it!' button.



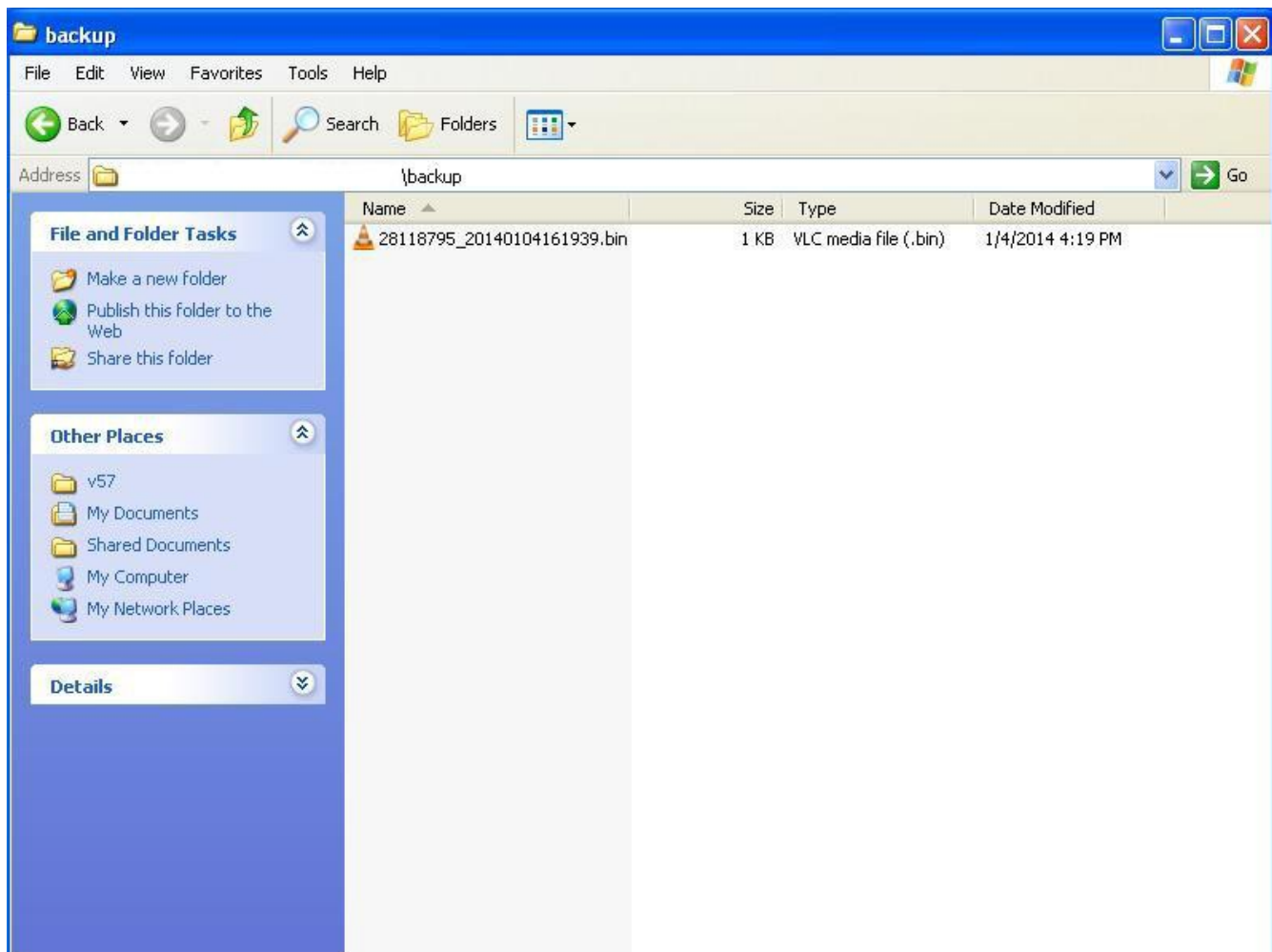
After it completes, the data is shown:



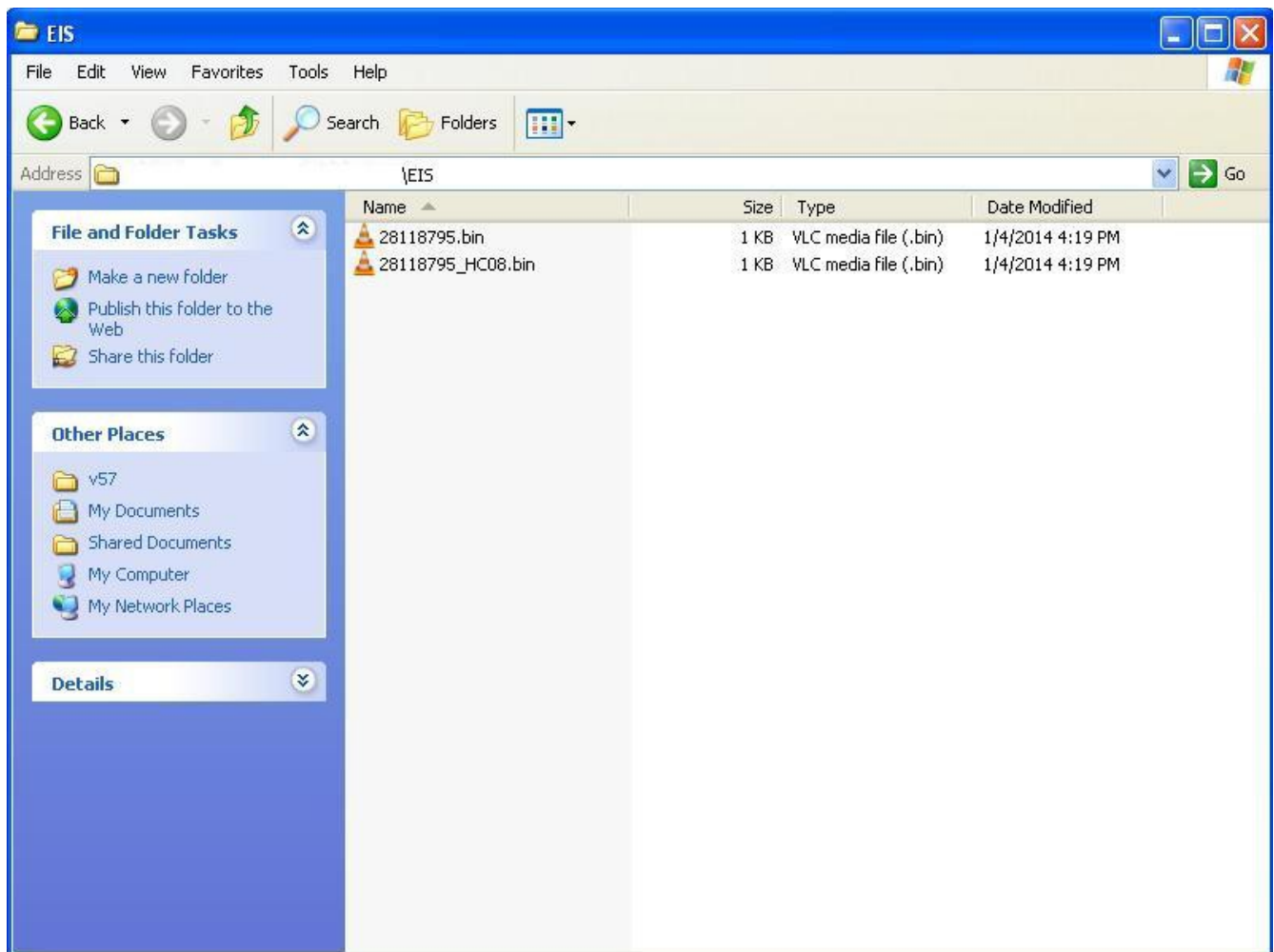
Note, that software shows You the data as it is - in plain format. You will find "Initial Hash" in the loaded Key file for writing in swapped format. This presentation of data in plain format is easier to accept, despite the fact that some Key generation applications and servers are treating Password and Hash data in it's swapped form.



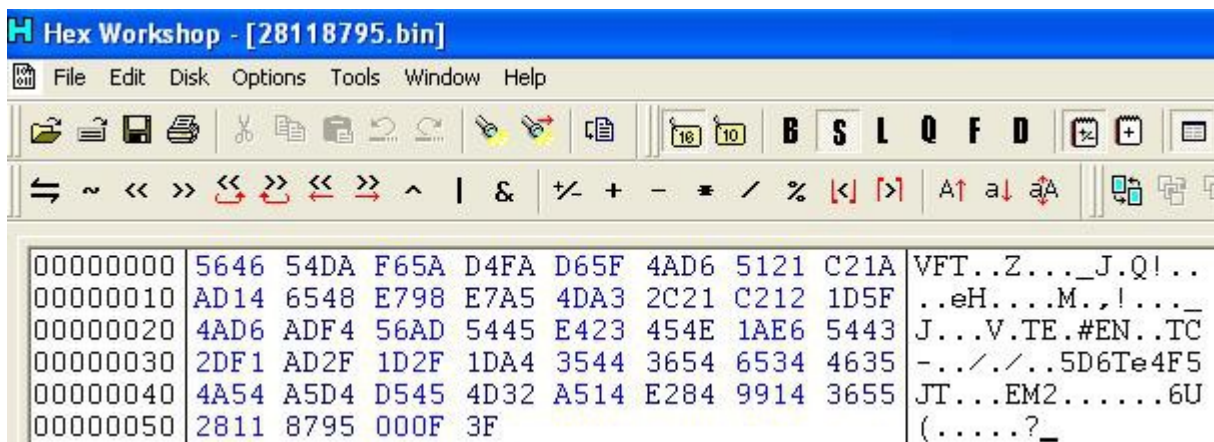
After above reading, software creates two folders (or re-uses files already present there) - “backup” and “EIS”. Files are created in sub-directories of current directory, where software is located. Files has unique name, containing SSID (unique 32-bit identifier) of Key and current date and time. This way You could read Key data many times without worrying of files being replaced by newer ones. So, no duplicate records will be stored in “backup” folder. By SSID or/and date/time, contained in file name, You could easy find record you need from all stored in backup directory and view it with binary editor software.



It is very important to note, that if You want to use the provided files for generation of new Keys or adaptation of ESL, then FIRST You should read EIS with IR Service Key and then read EIS Password. It is important order and should be obeyed in all cases, when You need complete “HC08”-format file for processing by standalone Key generation software. If You use online services, then that order is not important and You could process provided files further.

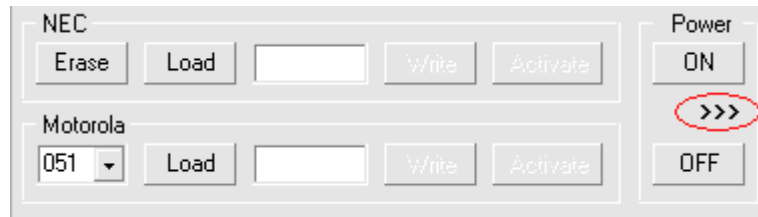


And here is how it looks the file for online server calculation from this folder:



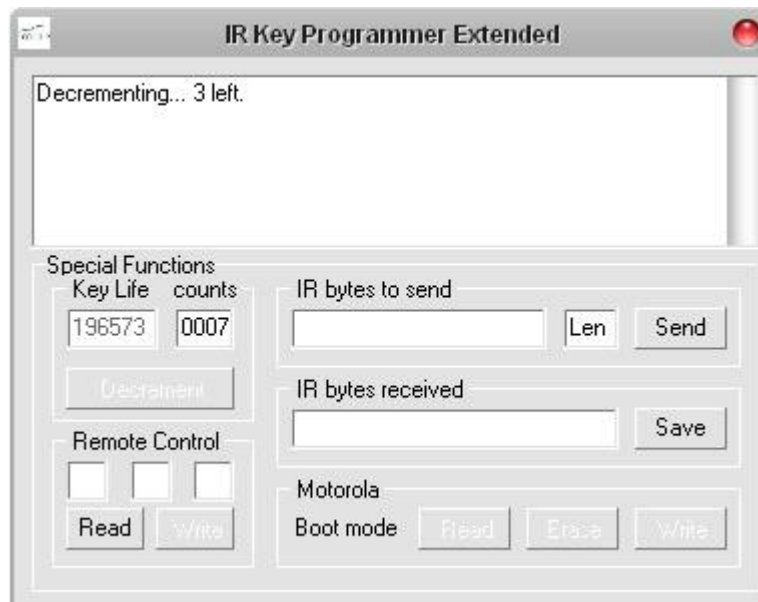
## Extended functions

Click “>>>” located between “ON” and “OFF” buttons (marked in red).



New window will open which allows decrementing of “Life” counter automatically and few other very helpful options like Motorola MCU read / write / erase, IR custom commands send / receive, etc...

If You wish to decrement key “Life” with big number (i.e. when exchanging old style big plastic keys to newer chromed design and You are using same Key number, same hashes, etc... from data, read by Motorola MCU with below shown button “Read” in Motorola Boot mode section), then enter number of counts to decrement in corresponding field and click “Decrement”. Software will inform You how tasks is progressing and screen will look like:

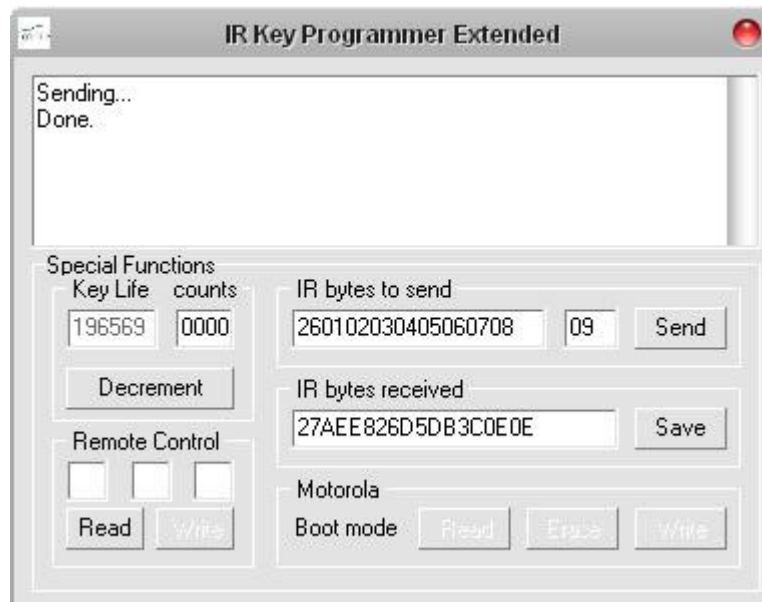


---

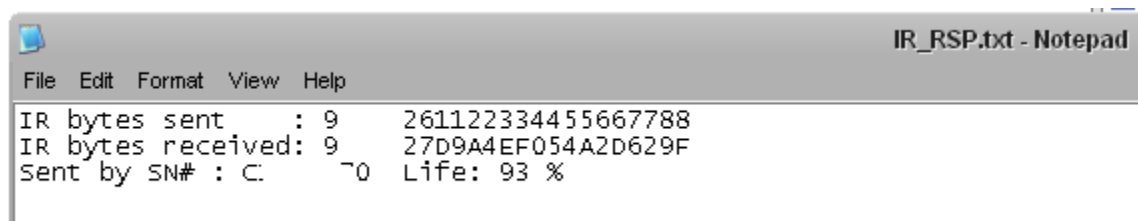
**Remark:** Mind EIS current hash “Life” counter when performing this operation.  
Another useful functionality is ability to send custom commands to MB key.

What should be written in “IR bytes to send” is command in hexadecimal format. Also number of bytes You want to send should be filled in decimal format into “Len” field. Clicking “Send” button results in transmitting of command via IR and receiving response if such exists. Not all possible commands have appropriate response. Be careful with that function – experimenting with MB key is fun, but consequences and responsibility are only Yours.

Example will be given for that functionality – as discussed above lifetime counter should be decremented. To simulate that MB Key is inserted into EIS, command “26” have to be send. Response “27” is received as shown below:



Clicking “Save” button will produce text file, logging request and response.

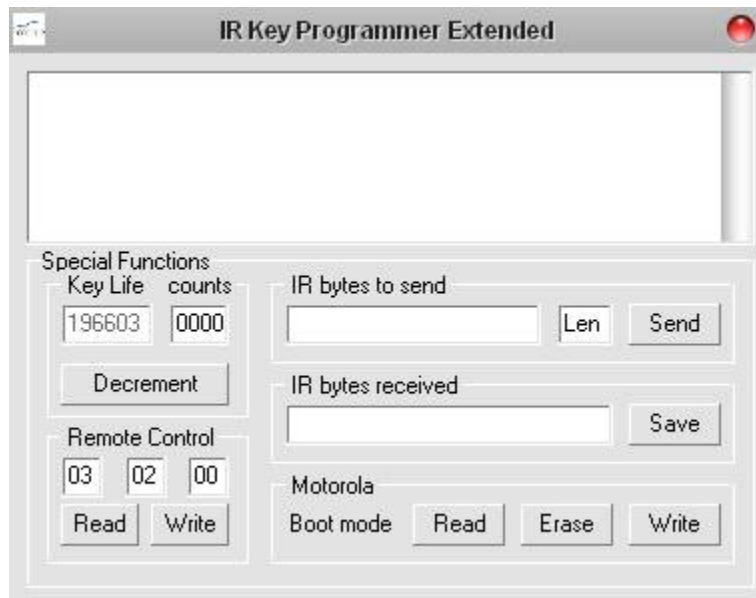


---

**Remark:** Some MB key models support different IR commands set. Results from Your experiments may vary with different MB key software versions and IR Key Programmer and its software are not to be blamed for any undesired effects.

Unique feature of our software, which You will not find amongst competitors is ability to repair NEC keys with not functioning radio part. This happens often after erasing and programming new dump to NEC key – key turns in EIS, car is started but remote control is inoperative.

Inside the key EPROM there are radio trimming bytes, which get destroyed when key is erased. With extended capabilities You are able to read and write those trimming bytes. At the below shown screenshot You could see the example result from reading working key:



Note that radio trimming bytes should be written **BEFORE** programming key dump to erased NEC MCU. First erase the MCU, check and correct radio trims and at last program key dump.

For radio to be operative, first byte should be „03“. Next two bytes are not so critical, but it's always good practice to have key read before erasure and restore same trimming values to it after erasing is completed. USA and EU models have different trimmings, which could vary from model to model, hence it's good practice to read keys prior to erasure and have database with possible values.

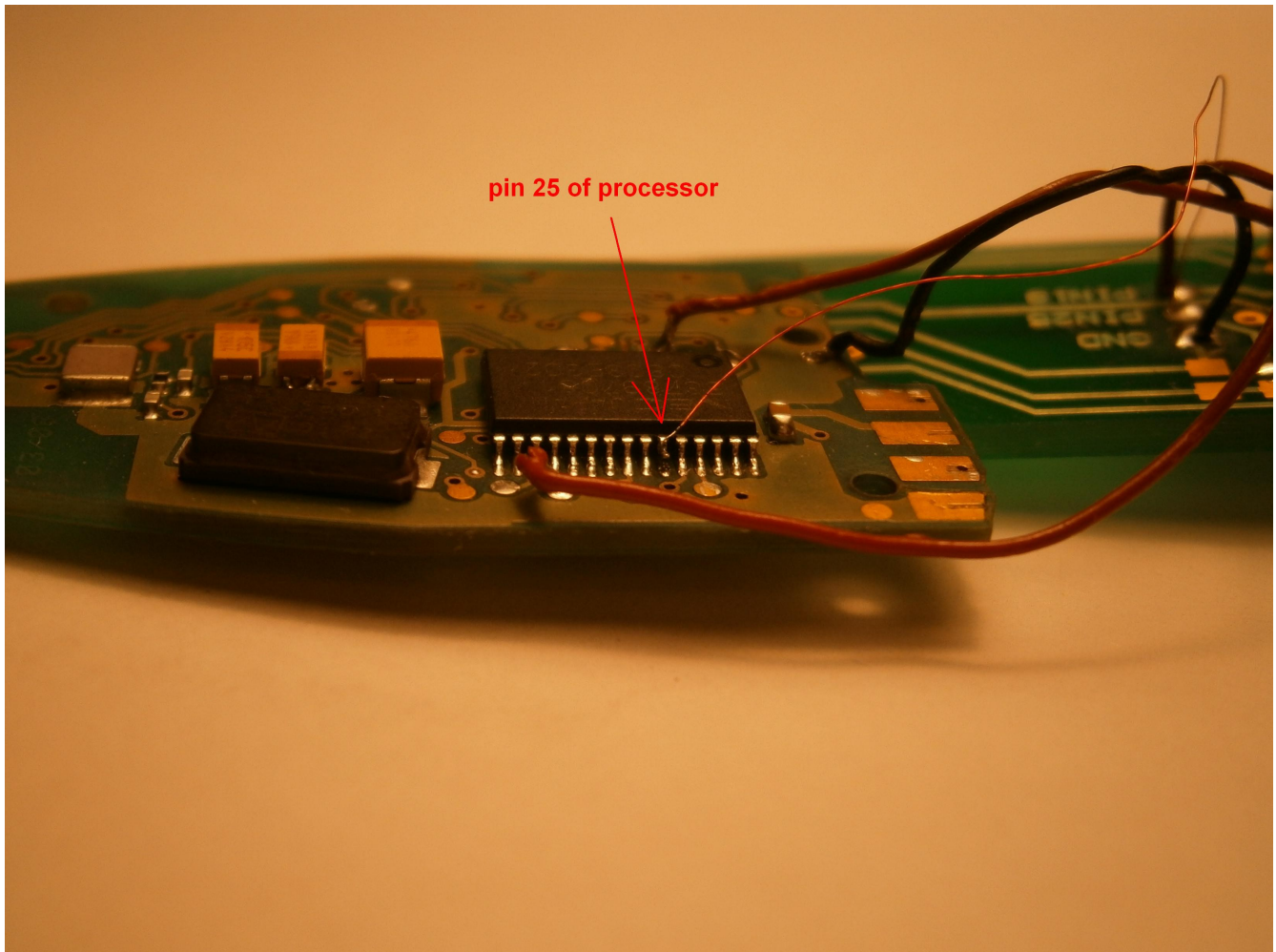
---

**Remark:** Remote Control trimming bytes are possible to write if NEC Key Status is „0000“. Follow above described erasure and reading techniques, until You achieve desired Key Status „0000“.



## Appendix A

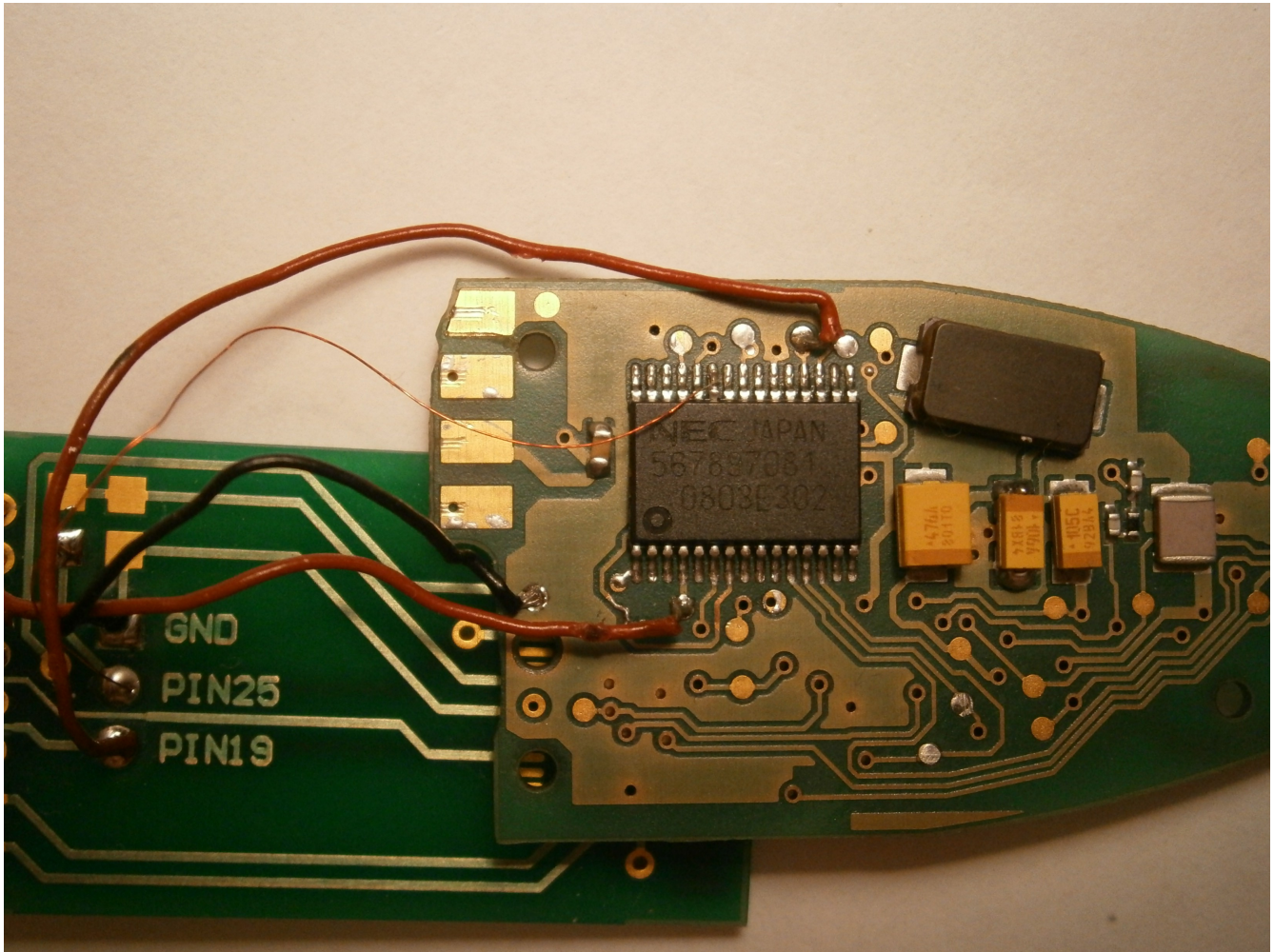
Erasing NEC MCU without desoldering it from key's PCB requires skills for connecting thin wires to processor pins. Do this with a lot of care! Use appropriate wires and tools. First desolder and lift a little bit pin 25 of MCU as shown:



After that solder thin wires from adapter board pads with corresponding names to pin 19, pin 25 of MCU and GND of PCB. For different models of key's PCB find correct spot to solder wires for GND and pin 19. On most of the models pin 19 has test pad routed to it and is not necessary to solder wire directly to this pin. Just locate where is it's test pad and solder wire there. Do not overheat MCU pins!

Locating GND (ground) is easy, so choose bigger wire for it to guarantee proper operation of device.

With all wires connected PCB has to look like (image is for reference only):



Now You are ready to connect adapter board to IR Key Programmer and perform erasure. On most of key's PCB models when erasing is completed key's LED blinks. You could observe it as with this erasing method software can't check if it's completed or not. For safer procedure solder MCU on adapter board!

**Always connect and disconnect adapter boards to programmer when USB cable is not plugged in !!!  
Serious damages could occur if IR Key Programmer is powered on while adapter board is being attached or removed !!! Do not avoid this warning !!!**

---

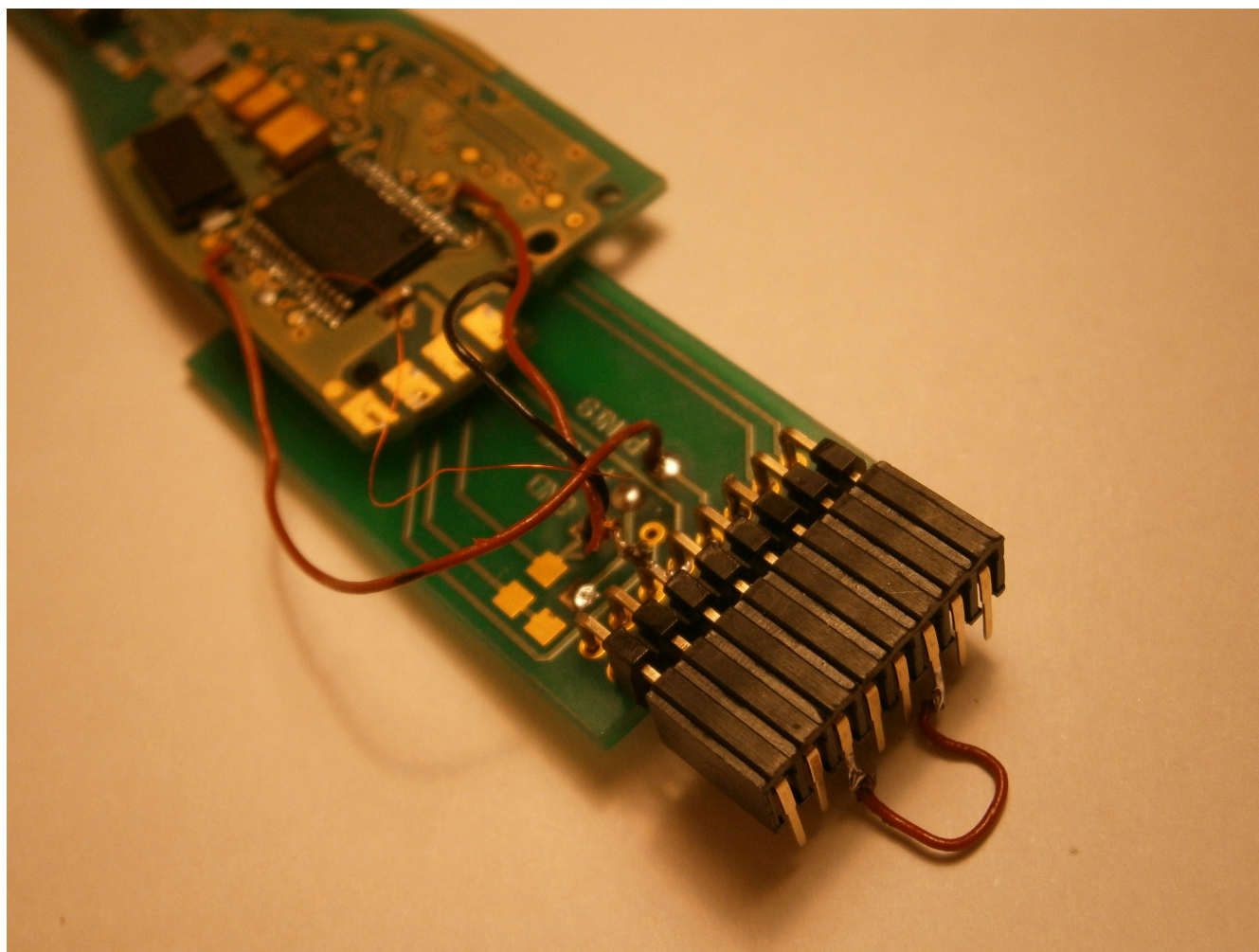
**Remark:** There is additional wire on above image, soldered to pin 4 of MCU. It's optional and for experienced users only! Read next page for more details!



If pin 4 of MCU is connected to pin 25 it allows to read / write key via IR port. It is not so safe as removing wires from it and putting PCB in it's enclosure, so do not try what is shown below if You are not sure You could keep key PCB in appropriate position and distance into IR Key Programmer.

Note that touching PCB with hand always impacts reliable operation and is not advisable. Also “playing” with PCB with soldered wires increases risk of short circuits and hence eventual damages.

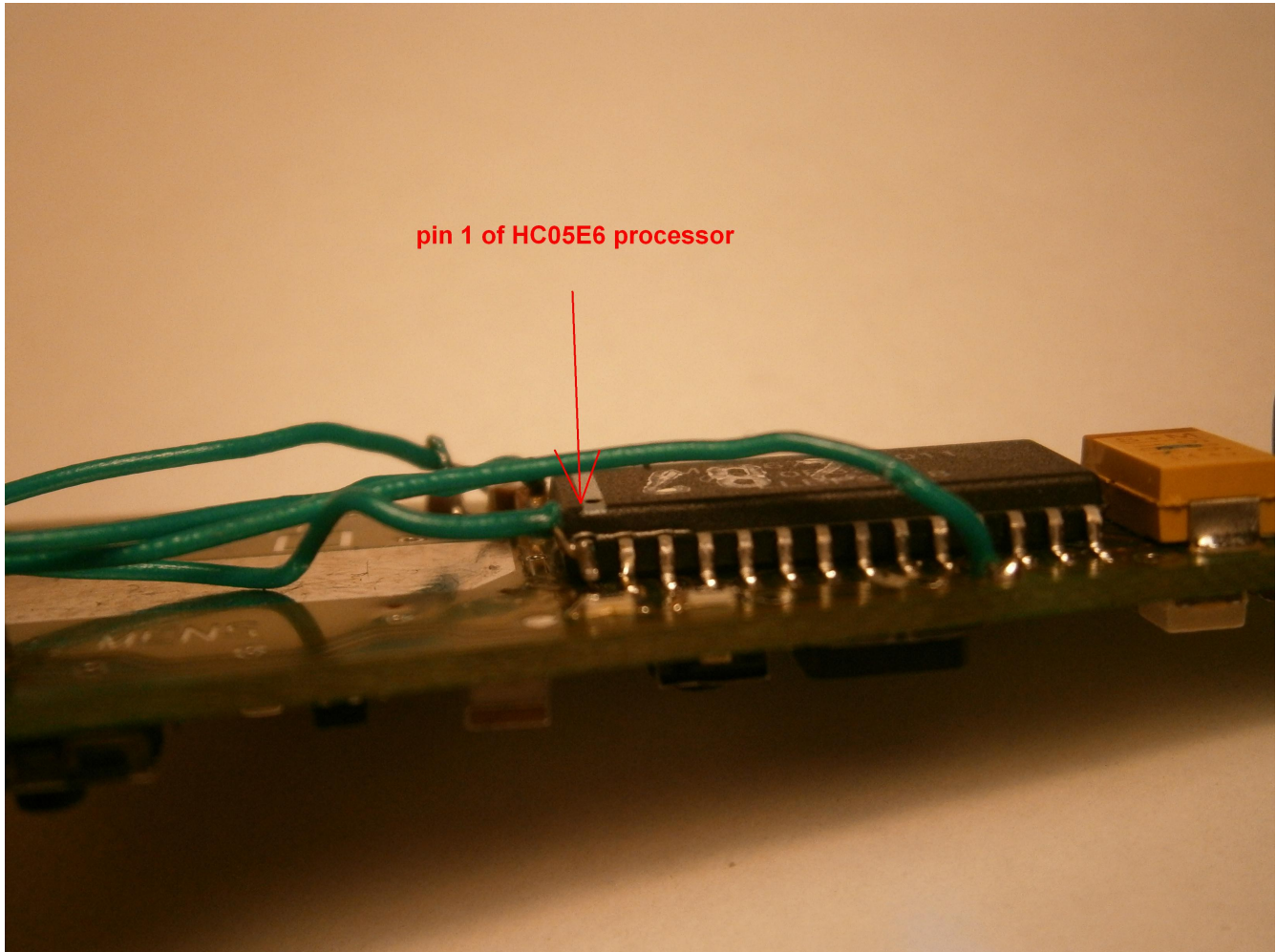
It is Your own risk to build below shown connector for using bare PCB as normal working via IR with inductive power from coil. No more explanations will be given – experienced user will not need any to understand purpose of this page. Non-experienced user should avoid fatal consequences of it's content ☺





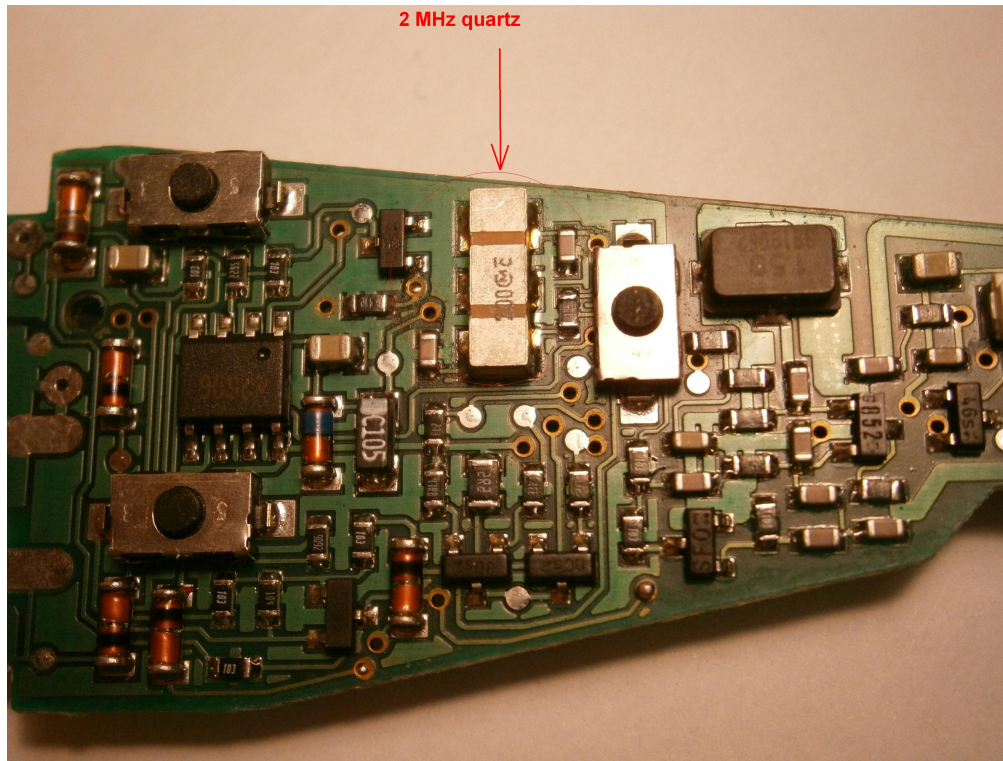
## Appendix B

Erasing Motorola MCU without desoldering it from key's PCB requires skills for connecting thin wires to processor pins. Do this with a lot of care! Use appropriate wires and tools. Desolder and lift a little bit pin 1 of MCU as shown:

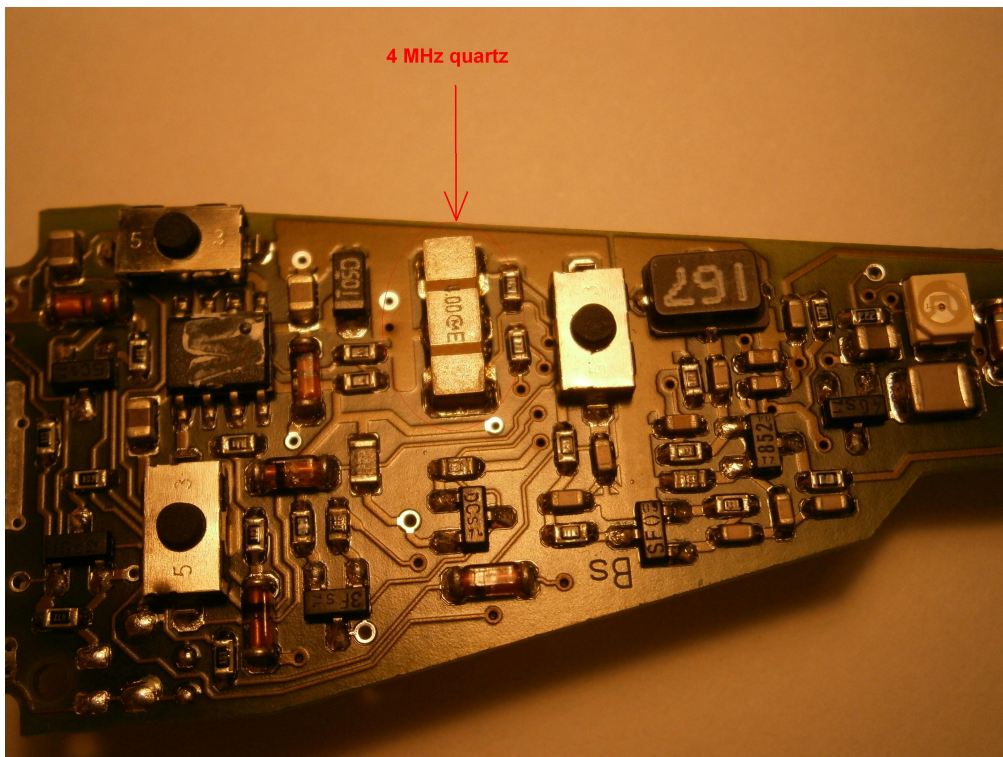


This operation carry eventual risk of damaging pin, so it is always advisable to solder Motorola on adapter for guaranteed results. Not only because of golden plated adapter PCB, which guarantees proper contact and long life of board, but also following processes of programming, activating, Life decreasing operations are faster with adapter. Also if You program wrong file into key it is very easy to erase it and reprogram with correct dump. Just after all tasks are finished and MCU is prepared for use in car, You could solder it back to key's PCB and make a final reading via IR before using with car.

Choose correct adapter board for 2 MHz or 4 MHz versions of MB Key.  
Markings on quartz resonator is visible and helps You identify it very easy on PCB.

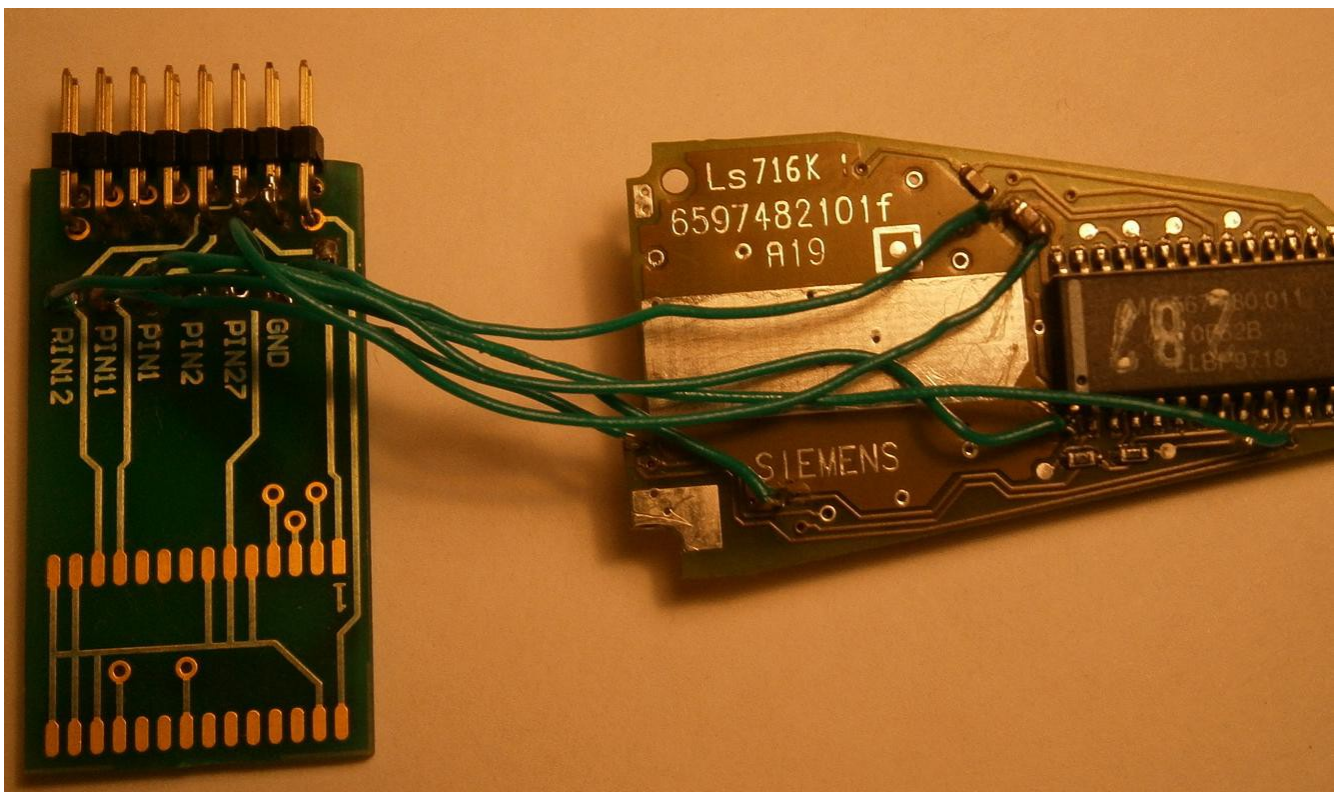
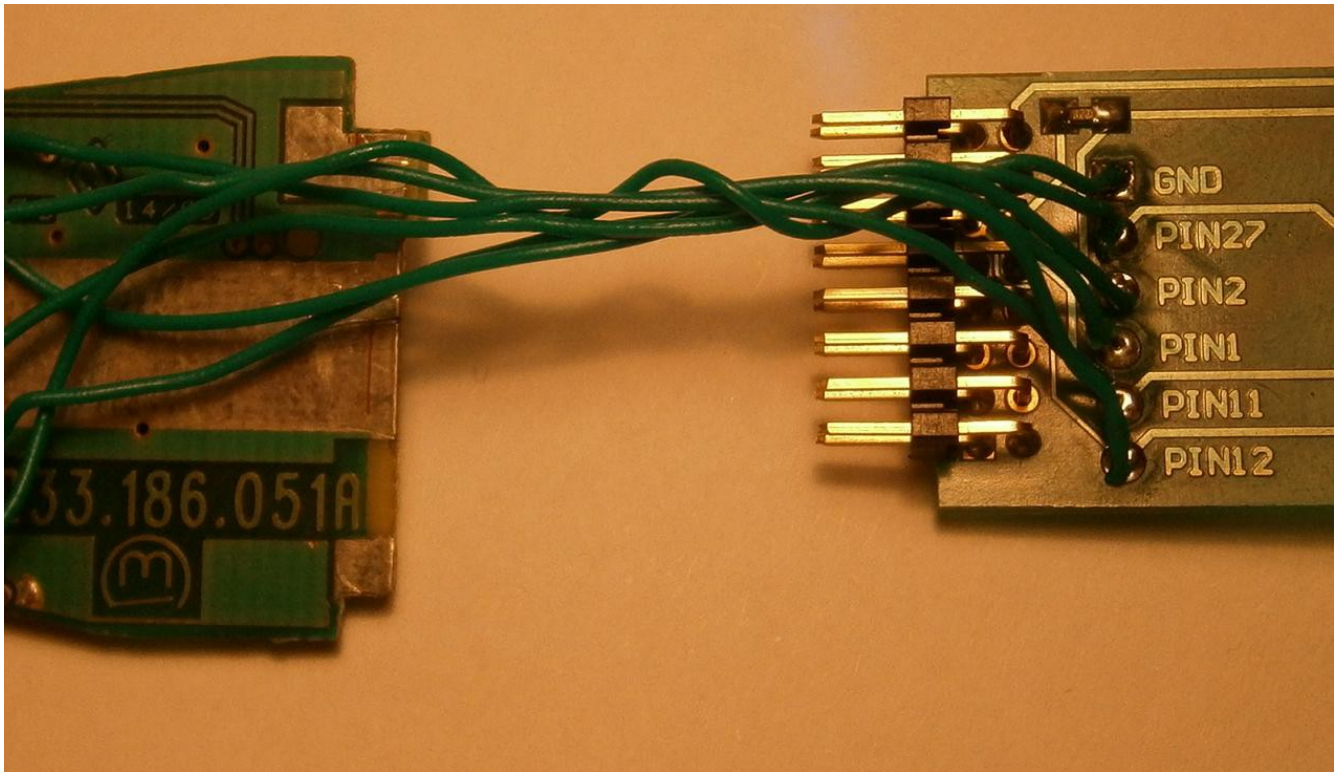


Images are for reference only and vary with different PCB hardware versions !



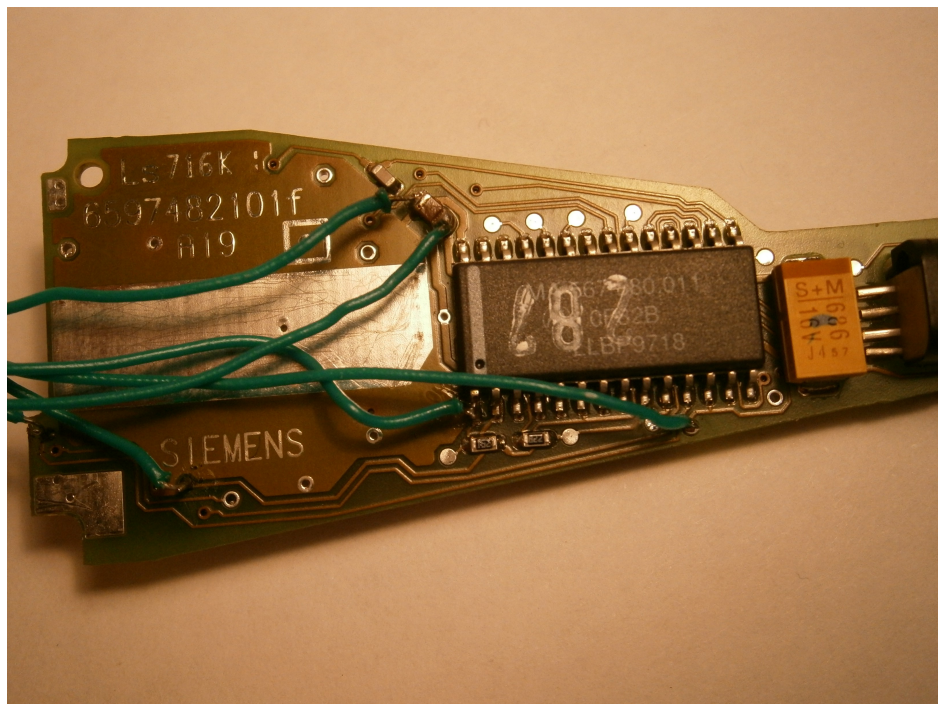
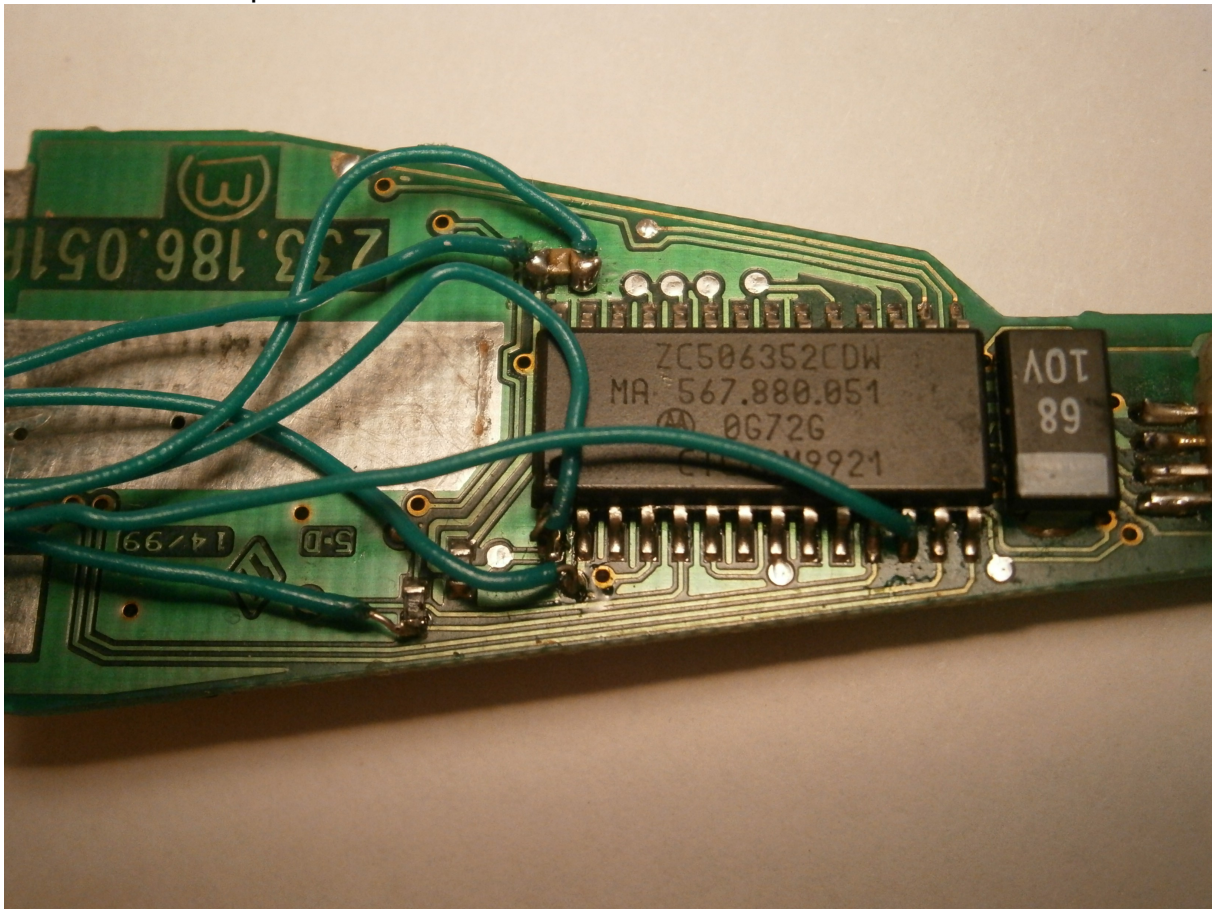


There are visible printings on adapter board to which MCU pin to solder corresponding pad. Keep wires as short as possible! Examples are shown below:





Here is example of 2 MHz PCB connections, and at the bottom is 4MHz PCB:



# Important Notice

**Always connect and disconnect adapter boards to IR Key Programmer with USB cable not plugged in !!!**

**The ONLY right way to connect adapter to IR Key Programmer is shown below. It doesn't matter if MCU is soldered directly on adapter or connected with wires. Orientation of adapter should be like this:**

